TABLE 2.—ROTORCRAFT CRITICAL DISPLAY FUNCTIONS FIELD STRENGTH VOLTS/METER—Continued

Frequency	Peak	Average
4 GHz–6 GHz ...	3000	200
6 GHz–8 GHz ...	1000	200
8 GHz–12 GHz	3000	300
12 GHz–18 GHz	2000	200
18 GHz–40 GHz	600	200

Applicability

As previously discussed, this special condition is applicable to the Bell Helicopter Model 429 helicopter. Should Bell Helicopter apply at a later date for a change to the type certificate to include another model incorporating the same novel or unusual design feature, the special condition would apply to that model as well under the provisions of § 21.101.

Conclusion

This action affects only certain novel or unusual design features on one model series of helicopters. It is not a rule of general applicability and affects only the applicant who applied to the FAA for approval of these features on the helicopter.

The substance of this special condition has been subjected to the notice and comment period previously and is written without substantive change from those previously issued. It is unlikely that prior public comment would result in a significant change from the substance contained in this special condition. For this reason, we have determined that prior public notice and comment are unnecessary, and good cause exists for adopting this special condition upon issuance. The FAA is requesting comments to allow interested persons to submit views that may not have been submitted in response to the prior opportunities for comment.

List of Subjects in 14 CFR Parts 21 and 27

Aircraft, Air transportation, Aviation safety, Rotorcraft, Safety.

■ The authority citation for these special conditions is as follows:

Authority: 42 U.S.C. 7572; 49 U.S.C. 106(g), 40105, 40113, 44701–44702, 44704, 44709, 44711, 44713, 44715, 45303.

The Special Condition

Accordingly, pursuant to the authority delegated to me by the Administrator, the following special condition is issued as part of the type certification basis for Bell Helicopter Model 429 helicopters.

Protection for Electrical and Electronic Systems from High Intensity Radiated Fields

1. Each system that performs critical functions must be designed and installed to ensure that the operation and operational capabilities of these critical functions are not adversely affected when the helicopter is exposed to high intensity radiated fields external to the helicopter.

2. For the purpose of this special condition, critical functions are defined as those functions, whose failure would contribute to, or cause, an unsafe condition that would prevent the continued safe flight and landing of the aircraft.

Issued in Fort Worth, Texas, on December 11, 2007.

Mark R. Schilling,

Acting Manager, Rotorcraft Directorate, Aircraft Certification Service.

[FR Doc. E7–25143 Filed 12–27–07; 8:45 am]

BILLING CODE 4910–13–P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Part 25

[Docket No. NM365 Special Conditions No. 25–357–SC]

Special Conditions: Boeing Model 787–8 Airplane; Systems and Data Networks Security–Protection of Airplane Systems and Data Networks from Unauthorized External Access

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Final special conditions.

SUMMARY: These special conditions are issued for the Boeing Model 787–8 airplane. This airplane will have novel or unusual design features when compared to the state of technology envisioned in the airworthiness standards for transport category airplanes. The architecture of the Boeing Model 787–8 computer systems and networks may allow access to external systems and networks, such as wireless airline operations and maintenance systems, satellite communications, electronic mail, the Internet, etc. On-board wired and wireless devices may also have access to parts of the airplane's digital systems that provide flight critical functions. These new connectivity capabilities may result in security vulnerabilities to the airplane's critical systems. For these design features, the applicable airworthiness regulations do not contain adequate or appropriate safety standards for protection and security of airplane systems and data networks against unauthorized access. These special conditions contain the additional safety standards that the Administrator considers necessary to establish a level of safety equivalent to that established by the existing standards. Additional special conditions will be issued for other novel or unusual design features of the Boeing Model 787–8 airplanes.

DATES: *Effective Date:* January 28, 2008.

FOR FURTHER INFORMATION CONTACT: Will Struck, FAA, Airplane and Flight Crew Interface, ANM–111, Transport Airplane Directorate, Aircraft Certification Service, 1601 Lind Avenue, SW., Renton, Washington 98057–3356; telephone (425) 227–2764; facsimile (425) 227–1149.

SUPPLEMENTARY INFORMATION:

Background

On March 28, 2003, Boeing applied for an FAA type certificate for its new Boeing Model 787–8 passenger airplane. The Boeing Model 787–8 airplane will be an all-new, two-engine jet transport airplane with a two-aisle cabin. The maximum takeoff weight will be 476,000 pounds, with a maximum passenger count of 381 passengers.

Type Certification Basis

Under provisions of 14 Code of Federal Regulations (CFR) 21.17, Boeing must show that Boeing Model 787–8 airplanes (hereafter referred to as ''the 787'') meet the applicable provisions of 14 CFR part 25, as amended by Amendments 25–1 through 25–117, except §§ 25.809(a) and 25.812, which will remain at Amendment 25–115. If the Administrator finds that the applicable airworthiness regulations do not contain adequate or appropriate safety standards for the 787 because of a novel or unusual design feature, special conditions are prescribed under provisions of 14 CFR 21.16.

In addition to the applicable airworthiness regulations and special conditions, the 787 must comply with the fuel vent and exhaust emission requirements of 14 CFR part 34 and the noise certification requirements of part 36. The FAA must also issue a finding of regulatory adequacy pursuant to section 611 of Public Law 92–574, the ''Noise Control Act of 1972.''

The FAA issues special conditions, as defined in § 11.19, under § 11.38, and they become part of the type certification basis under § 21.17(a)(2).

Special conditions are initially applicable to the model for which they are issued. Should the type certificate

for that model be amended later to include any other model that incorporates the same or similar novel or unusual design feature, the special conditions would also apply to the other model under § 21.101.

Novel or Unusual Design Features

The digital systems architecture for the 787 consists of several networks connected by electronics and embedded software. This proposed network architecture is used for a diverse set of functions, including the following.

1. Flight-safety-related control and navigation and required systems (Aircraft Control Domain).
2. Airline business and administrative support (Airline Information Domain).
3. Passenger entertainment, information, and Internet services (Passenger Information and Entertainment Domain).

The proposed architecture of the 787 is different from that of existing production (and retrofitted) airplanes. It may allow connection to and access from external sources and airline operator networks to the previously isolated Aircraft Control Domain and Airline Information Domain. Types of connections and access from external sources may include wireless systems, satellite communications, electronic mail, the Internet, etc. The Aircraft Control Domain and the Airline Information Domain perform functions required for the safe operation of the airplane.

Capability is proposed for providing electronic transmission of field-loadable software applications and databases to the aircraft. These would subsequently be loaded into systems within the Aircraft Control Domain and Airline Information Domain. Also, it may be proposed that on-board wired and wireless devices have access to the Aircraft Control Domain and Airline Information Domain. These new connectivity capabilities and features of the proposed design may result in security vulnerabilities from intentional or unintentional corruption of data and systems critical to the safety and maintenance of the airplane. Existing regulations and guidance material did not anticipate this type of system architecture or Internet and wireless electronic access to aircraft systems that provide flight critical functions. Furthermore, 14 CFR regulations and current system safety assessment policy and techniques do not address potential security vulnerabilities that could be caused by unauthorized external access to aircraft data buses and servers. Therefore, special conditions are proposed to ensure the security, integrity, and availability of the critical systems within the Aircraft Control Domain and the Airline Information Domain by establishing requirements for:

1. Protection of Aircraft Control Domain and Airline Information Domain systems, hardware, software, and databases from unauthorized access.
2. Protection of field-loadable software (FLS) applications and databases that are electronically transmitted from external sources to the on-aircraft networks and storage devices, and used within the Aircraft Control Domain and Airline Information Domain.
3. Test and evaluation of security protection means and change control procedures of aircraft systems, hardware, software, and databases, especially for critical systems and those areas that could affect safety of flight.

Discussion Of Comments

Notice of Proposed Special Conditions No. 25–07–02–SC for the 787 was published in the **Federal Register** on April 16, 2007 (72 FR 18923). Several comments were received from Airbus.

• *AIRBUS General Comment 1:* In Airbus's opinion these special conditions leave too much room for interpretation, and related guidance and acceptable means of compliance should be developed in an advisory circular (AC) for use by future applicants.

FAA Response: We agree that guidance is necessary. Detailed guidelines and criteria have been developed for this aircraft certification program, specific to this airplane's network architecture and design, providing initial guidance on an acceptable means of compliance for the 787. Additionally, the FAA intends to participate in an industry committee chartered with developing acceptable means of compliance to address aircraft network security issues, and hopes to endorse the results of the work of that committee by issuing an AC. Until such time as guidance is developed for a general means of compliance for network security protection, these special conditions and the agreed-to guidance are imposed on this specific network architecture and design. We have made no changes to these special conditions as a result of this comment.

• *AIRBUS Comment (a):* Airbus said that the meaning of ''shall ensure system security protection * * * from unauthorized external access'' in the first sentence is not accurate enough. Airbus commented that this could be interpreted as a zero allowance and demonstrating compliance with such a requirement all through the aircraft's life cycle is quite impossible since security threats evolve very rapidly. The commenter maintained that the only possible solution to such a requirement would be no link and no communication at all between the aircraft and the outside world. Airbus asked, ''if some residual vulnerabilities are allowed, which criteria have to be used to assess their acceptability?''

FAA Response: The applicant is responsible for the design of the airplane network and systems architecture and for ensuring that potential security vulnerabilities of providing external access to airplane networks and systems are mitigated to an appropriate level of assurance, depending on the potential risk to the airplane and occupant safety. This responsibility is similar to that entailed in the current system safety assessment process of 14 CFR 25.1309. (See also AC 25.1309–1A and the ARAC-recommended Arsenal version of this AC, at *http://www.faa.gov/regulations_policies/rulemaking/committees/arac/media/tae/TAE_SDA_T2.pdf* and SAE ARP 4754). These special conditions do not prescribe a specific level of assurance because assurance levels are dependent on the aircraft network architecture, specific external access points allowed, potential threats and vulnerabilities of each access, and various means of mitigating those vulnerabilities, whether by aircraft and network design features, monitoring features, operational procedures, maintenance procedures, and/or combinations thereof. Detailed compliance guidelines and criteria, specific to the 787 network architecture and design, have been developed to provide initial guidance for an acceptable means of compliance for this aircraft model. Residual vulnerabilities may have to be assessed on a case-by-case basis to ascertain whether sufficient and acceptable mitigation is provided. As mentioned earlier, the FAA intends to participate in an industry forum chartered with determining appropriate criteria and acceptable means of compliance, and hopes to endorse that guidance with an AC. We have made no changes to these special conditions as a result of this comment.

• *AIRBUS Comment (b):* Airbus commented that external access can be interpreted in two ways: external to the aircraft, or external to the Aircraft Control Domain and Airline Information Domain. It said that the Passenger Information and Entertainment Domain (PIED) may be considered external and,

if it is, this special condition is redundant to Proposed Special Condition 25–07–01–SC.

FAA Response: Since these special conditions are applicable to the 787 aircraft, the interpretation of ''external'' means external to the 787 aircraft. Although the PIED is external to the other domains mentioned, it is ''internal'' to the aircraft. Special Condition 25–07–01–SC was developed to address interfaces between the PIED and the Aircraft Control and Airline Information Domains, and is therefore not redundant. We have made a minor change to these special conditions as a result of this comment. We have reworded the special conditions, changing the words ''unauthorized external access'' to ''access by unauthorized sources external to the airplane'' in order to clarify this point.

• *AIRBUS Comment (c):* Airbus commented that the term ''unauthorized external access'' is too vague and could be interpreted in too restrictive a way, resulting in too few threats being considered. The commenter asked whether unauthorized external access encompasses physical access or unauthorized access by an authorized user and/or an unauthorized user. The commenter asked whether physical tampering has to be considered. Airbus suggested that any threats external to the aircraft be considered, and that we refer as well to the list of threats in the National Airspace System Communication System Safety Hazard Analysis and Security Threat Analysis.

FAA Response: The applicant is responsible for the aircraft network architecture and design, and for implementing security protection mechanisms and controls. Examples include:

• defining authorized versus unauthorized users,

• user authentication,

• defining the scope of authorized users' access to various components connected to the airplane networks,

• ensuring correct software loads are stored on appropriately secured servers, are loaded into the correct systems, are compatible with other loads, etc.; and

• defining the maintenance requirements for ensuring continued operational safety of the aircraft.

Operators and maintainers are responsible for performing maintenance procedures in compliance with those requirements. For maintenance tasks, however, it may be appropriate to provide some level of security protection for mechanics to ensure they are authorized for specific tasks within certain domains or systems of the aircraft for performing repairs or loading software updates, which would typically require ''physical access.'' With current wireless technology, actual physical access may not be necessary to perform some maintenance functions. The applicant is responsible for developing a design which complies with these special conditions and other applicable regulations. The design may include specific technology and architecture features as well as operator requirements, operational procedures and security measures, and maintenance procedures and requirements to ensure an appropriate implementation that can be properly used and maintained to ensure safe operations and continued operational safety. Applicants should define all external accesses and the scope of their aircraft network security protections. Use of the threats listed in the above-mentioned document may be appropriate for these purposes. We have made no changes to these special conditions as a result of this comment.

• *AIRBUS Comment (d):* Airbus said that the external environment needs to be characterized in order to determine which threats the Aircraft Control Domain and Airline Information Domain must be protected from. Questions to be answered include who can and cannot access; who is and is not trusted; and what threat source profile must be considered. The commenter asked whether only new communication media (like internet protocol (IP) communications) would be considered not trusted, or whether all communications, including existing communications for which no security requirements have been applied up to now, would be considered not trusted. Airbus gave ACARS (the Aeronautical Radio Incorporated Communication Addressing and Reporting System) as an example of existing communications that currently have no security requirements.

FAA Response: Each access (or communication) from an external source and its potential vulnerabilities to threats should be evaluated. The security mitigation should provide protection to an appropriate level, whether by design, monitoring, operational procedures, or other means. The security solution could certainly consider access rights and scope, trusted versus not trusted sources and data, how reliable incoming communication data may be, and other factors, depending on the intended use and potential for presenting a security risk. We have made no changes to these special conditions as a result of this comment.

• *AIRBUS Comment (e):* Airbus said that the characterization of the external environment must be extended to the maintenance organization, because the security objectives of these special conditions must consider maintenance activity. Proposed condition 1 requires minimizing the likelihood of reductions in safety margins or airplane functional capabilities, ''* * * including those possibly caused by maintenance activity''. Airbus said that the trust level for the maintenance organization, to be defined, may significantly impact the design of the on-board security protections and the compliance demonstration.

FAA Response: The proposed special conditions include the potential for security risks from maintenance activities. Applicants should develop a design and maintenance procedures which facilitate routine maintenance of the aircraft, networks and systems, and equipment. The design and maintenance procedures should also provide capabilities for ensuring that security features and updates can be maintained by the operators and maintenance personnel, to ensure continued airworthiness and operational safety of the aircraft for its service life. These are methods of compliance issues, and therefore we have made no changes to these special conditions as a result of this comment.

• *AIRBUS Comment (f):* Airbus referred to wording in the second sentence of the proposed special condition : ''* * * to minimize the likelihood of occurrence of each of the following conditions: * * * '' Airbus noted that the definition of likelihood of occurrence and the criteria for fulfilling the security objectives are missing. The commenter asked, ''when is an identified risk considered mitigated?'' Airbus also noted that the 3 conditions at the end of the special conditions are quite similar to the description of safety severity effects for a ''Failure Condition classified Major'' per AC 25.1309–1A (or AC/AMJ No: 25.1309). Airbus maintained that, as a result, this description can be interpreted as an allowable qualitative likelihood of occurrence corresponding to ''remote'' and an allowable quantitative probability corresponding to less than 10E–5. Airbus said that such a classification, if interpreted in this way, may be irrelevant in some cases, because consequences may be more severe, and only a security threat analysis process can conclude which safety effect is acceptable. The commenter said that recognizing this process as an acceptable means of compliance (through an AC) could

remove any dispute about how to assess the severity and likelihood of occurrence of a threat over which the applicant has no control.

FAA Response: We agree that a ''security threat analysis process'' (or other acceptable means) should be conducted to determine the threats, vulnerabilities, and risks of each airplane network access from an external source to determine appropriate security mitigation protection and procedures for the aircraft, its operations, and maintenance. The aircraft and system safety assessments (as described in AC 25.1309) should certainly consider the impact of security vulnerabilities on aircraft safety and the capabilities of the aircraft's systems to satisfy reliability and integrity requirements. Detailed guidelines and criteria, specific to the 787 network architecture and design, have been developed for this aircraft and provide some initial guidance for an acceptable means of compliance. The FAA also intends to participate in industry efforts to develop additional guidance on the scope of security assessments and a general means of addressing aircraft network security concerns. We hope to endorse the industry-developed guidance, when it has been completed, with an advisory circular. We have made some minor changes to these special conditions as a result of this comment to clarify the scope for security threat analysis.

• *AIRBUS proposed text revision:* Airbus proposed the following revised wording for these special conditions.

The applicant shall ensure that security threats external to the aircraft (including those possibly caused by maintenance activity) are assessed and risk mitigation strategies are implemented to protect the Aircraft Control Domain and Airline Information Services Domain from adverse impacts reducing the aircraft safety.

FAA Response: Airbus's comments and proposal have merit but the proposal does not address all of the FAA concerns. We have, however, adopted several aspects of the commenter's proposal into these final special conditions. We have made these wording changes for clarification, but the meaning and intent of these special conditions remain the same as originally proposed.

Applicability

As discussed above, these special conditions are applicable to the 787. Should Boeing apply at a later date for a change to the type certificate to include another model on the same type certificate incorporating the same novel or unusual design features, these special conditions would apply to that model as well.

Conclusion

This action affects only certain novel or unusual design features of the 787. It is not a rule of general applicability.

List of Subjects in 14 CFR Part 25

Aircraft, Aviation safety, Reporting and recordkeeping requirements.

The authority citation for these special conditions is as follows:

Authority: 49 U.S.C. 106(g), 40113, 44701, 44702, 44704.

The Special Conditions

Accordingly, pursuant to the authority delegated to me by the Administrator, the following special conditions are issued as part of the type certification basis for the Boeing Model 787–8 airplane.

The applicant shall ensure system security protection for the Aircraft Control Domain and Airline Information Domain from access by unauthorized sources external to the airplane, including those possibly caused by maintenance activity. The applicant shall ensure that security threats are identified and assessed, and that risk mitigation strategies are implemented to protect the airplane from all adverse impacts on safety, functionality, and continued airworthiness.

Issued in Renton, Washington, on December 17, 2007.

Ali Bahrami,

Manager, Transport Airplane Directorate, Aircraft Certification Service.

[FR Doc. E7–25075 Filed 12–27–07; 8:45 am]

BILLING CODE 4910–13–P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Part 25

[Docket No. NM385; Special Conditions No. 25–364–SC]

Special Conditions: Boeing Model 757 Series Airplanes; Seats With Non-Traditional, Large, Non-Metallic Panels

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Final special conditions.

SUMMARY: These special conditions are issued for Boeing Model 757 Series Airplanes. These airplanes, as modified by Triad International Maintenance Company (TIMCO), will have a novel or unusual design feature(s) associated with seats that include non-traditional, large, non-metallic panels that would affect survivability during a post-crash fire event. The applicable airworthiness regulations do not contain adequate or appropriate safety standards for this design feature. These special conditions contain the additional safety standards that the Administrator considers necessary to establish a level of safety equivalent to that established by the existing airworthiness standards.

DATES: Effective Date: The effective date of these special conditions is December 18, 2007.

FOR FURTHER INFORMATION CONTACT: Dan Jacquet, FAA, Airframe/Cabin Safety Branch, ANM–115, Transport Airplane Directorate, Aircraft Certification Service, 1601 Lind Avenue, SW., Renton, Washington, 98057–3356; telephone (425) 227–2676; facsimile (425) 227–1232; electronic mail *daniel.jacquet@faa.gov.*

SUPPLEMENTARY INFORMATION:

Future Requests for Installation of Seats with Non-Traditional, Large, Non-Metallic Panels

We anticipate that seats with non-traditional, large, non-metallic panels will be installed in other makes and models of airplanes. We have made the determination to require special conditions for all applications requesting the installation of seats with non-traditional, large, non-metallic panels until the airworthiness requirements can be revised to address this issue. Having the same standards across the range of airplane makes and models will ensure a level playing field for the aviation industry.

Background

On July 31, 2007, Triad International Maintenance Company (TIMCO), 623 Radar Road, Greensboro, North Carolina 27410, applied for a supplemental type certificate for installing seats that include non-traditional, large, non-metallic panels in a Boeing Model 757 series airplane. The Boeing Model 757 series airplanes, currently approved under Type Certificate No. A2NM, are swept-wing, conventional tail, twin-engine, turbofan-powered, single aisle, medium-sized transport category airplanes.

The applicable regulations to airplanes currently approved under Type Certificate No. A2NM do not require seats to meet the more stringent flammability standards required of large, non-metallic panels in the cabin interior. At the time the applicable rules were written, seats were designed with a metal frame covered by fabric, not with large, non-metallic panels. Seats also met the then recently adopted standards for flammability of seat